

A person in a white shirt is holding a smartphone in their right hand, looking at the screen. The phone is held over a document that features various charts and graphs. A blue pen is resting on the document. The background is a blurred office setting with a yellow wall and a door.

Regimento da Auditoria Interna da **BB Previdência**

Índice

Introdução	4
Propósito	4
Missão	4
Parte 1 - Auditoria	5
1 Histórico	5
2 Conceitos	5
2.1 Auditoria Externa	5
2.2 Auditoria Interna	6
3 O Auditor Interno	7
3.1 Ética para o Auditor Interno	7
3.2 Papel do Auditor Interno	9
3.3 Qualidades Inerentes ao Auditor Interno	10
3.4 Postura do Auditor Interno	11
4 Auditoria Interna da BB Previdência	13
4.1 Governança	13
4.2 Posicionamento da Auditoria Interna na Organização	13
4.3 Objetivos e estrutura da Auditoria Interna	15
4.4 Responsabilidades	15
5 Auditoria Integrada	17
5.1 O que é?	17
5.2 Pilares da Auditoria Integrada	19
5.3 Auditoria Baseada em Riscos - ABR	19
5.4 Abordagem por Macroprocessos Críticos - AMC	20
6 Categorias de atividades de Auditoria Interna	21
6.1 Auditorias Programadas	21
6.1.1 Macroprocessos Críticos	22
6.1.2 Auditorias Corporativas	23
6.1.3 Auditorias Obrigatórias	23
6.1.4 Demandas Extraordinárias	23
6.1.5 Projetos	23
Parte 2 - Metodologia de Auditoria Interna	24

1	Processo de Auditoria.....	24
1.1	Princípios do Processo	24
1.2	Plano Anual de Auditoria Interna	25
1.3	Pré-Auditoria	26
1.3.1	O que é?	26
1.3.2	Objetivos	28
1.3.3	Levantamento e análise de dados	29
1.3.4	Mapeamento e Mapas	30
1.3.5	Amostragem	30
1.3.6	Instrumental de Auditoria	31
1.3.6.1	Papel de Trabalho - PT	31
1.3.6.2	Papel de Trabalho Auxiliar – PT Auxiliar	31
1.3.6.3	Orientações Gerais	32
1.4	Execução.....	32
1.4.1	O que é?	32
1.4.2	Aplicação de testes.....	33
1.4.3	Indicadores.....	33
1.4.4	Achados de Auditoria	33
1.4.5	Registros de Fragilidade e Lista de Falhas.....	34
1.4.6	Recomendação	35
1.4.6.1	Recomendação tipo plano de ação.....	36
1.5	Comunicação de Resultados.....	36
1.5.1	Relatório de Auditoria	37
1.5.2	Súmula de Trabalho de Auditoria	38
1.6	Pós Auditoria	38
2	Auditoria Contínua	38
2.1	Estratégia de Auditoria Contínua.....	39
2.2	Obtenção dos dados	39
2.3	Indicadores de Auditoria Contínua	40
2.4	Comunicação de Resultados e Monitoramento.....	40

Introdução

Este Regimento apresenta os elementos que orientam o trabalho da Auditoria Interna da BB Previdência, e é constituído de três partes.

Nesta primeira parte são apresentados o propósito e a missão da Auditoria Interna. Na segunda são apresentados o conceito e os tipos de auditoria, seus elementos formadores e os orientadores para atuação do auditor interno. Na terceira parte é apresentada a metodologia utilizada pela Auditoria Interna da BB Previdência. Importante ressaltar que esta metodologia é aderente às Normas e Orientações - Estrutura Internacional de Práticas Profissionais (IPPF), que é a base conceitual que organiza as informações oficiais promulgadas pelo *The Institute of Internal Auditors* (IIA)¹

Propósito

O propósito da Gerência de Auditoria Interna (Geaud) da BB Previdência é oferecer serviços objetivos de avaliação e consultoria, desenvolvidos para agregar valor e melhorar as operações da Entidade.

Missão

A missão da Auditoria Interna é aumentar e proteger o valor organizacional, fornecendo avaliações, assessoria e conhecimento objetivos baseados em risco. A Geaud auxilia a BB Previdência a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, gerenciamento de riscos e controles.

¹ *The Institute of Internal Auditors* é uma associação profissional internacional com sede nos Estados Unidos, organizada em 1941, para desenvolver a condição profissional da auditoria interna. Suas orientações são reconhecidas como as mais avançadas na área de auditoria interna.

Parte 1 - Auditoria

1 Histórico

Etimologicamente a palavra “auditoria” tem a sua origem no verbo latino *audire*, que significa “ouvir”, e que conduziu à criação da palavra “auditor” (do latim *auditor*) como sendo aquele que ouve. Isto pelo fato de, nos primórdios da auditoria, os auditores tirarem as suas conclusões fundamentadamente com base nas informações verbais que lhes eram transmitidas.

A função auditoria nasceu em épocas remotas e evoluiu com o avanço da civilização, na medida em que surgia a necessidade de verificação da fidelidade da gestão sobre a propriedade. Existem registros arqueológicos de inspeção e verificações na antiga Suméria que datam de 4.500 anos a.C. Na China, no Egito e na Grécia já eram realizadas inspeções nas contas de funcionários públicos e na arrecadação de impostos. Também existem registros de práticas de auditoria realizadas nas províncias romanas.

Com o advento da revolução industrial surgiram as grandes plantas fabris, construídas com dinheiro de vários investidores. Esta dualidade (investidor e operador da indústria) trouxe a necessidade de uma avaliação imparcial, focada principalmente na detecção de fraudes e erros; de onde surgiram as bases da auditoria moderna.

Atualmente, atribuiu-se à auditoria um conjunto mais abrangente de importantes funções, envolvendo todo o organismo da entidade e dos seus órgãos de gestão, com a finalidade de efetuar críticas e emitir opiniões sobre a situação econômico-financeira e sobre os resultados de ambos. Ressalte-se que a auditoria também tem o objetivo de identificar deficiências no sistema de controle interno e nos relatórios financeiros, apresentando recomendações para melhorá-los.

2 Conceitos

2.1 Auditoria Externa

Auditoria externa ou auditoria independente constitui o conjunto de procedimentos técnicos que tem por objetivo a emissão de parecer sobre a adequação das demonstrações contábeis, consoante os Princípios Fundamentais de Contabilidade, as Normas Brasileiras de Contabilidade e a legislação específica. (Normas Brasileiras de Contabilidade, NBC T-11).

A obrigatoriedade de contratação de serviços de auditoria independente pelas companhias abertas é exigida pela Lei 6.404 (art. 177, parágrafo 3º). A obrigação das Empresas Fechadas de Previdência Complementar é regulamentada pela Resolução CNPC nº 8, de 31.10.2011. O Manual de Governança da BB Previdência prevê que:

"A Auditoria Independente tem a responsabilidade técnica de avaliação da gestão econômico-financeira e da sua fiel retratação na contabilidade e nas demonstrações contábeis. Tem também a responsabilidade pela avaliação dos procedimentos, operacionais e de controle."

2.2 Auditoria Interna

A atividade de auditoria interna tem uma abrangência maior do que a exercida pelos auditores externos. O auditor interno pertence à entidade que audita, diferentemente do auditor externo. Enquanto este tem seu foco na fidedignidade dos relatórios, o auditor interno preocupa-se com o sucesso e perpetuidade da instituição onde atua. A Auditoria Interna é uma atividade exercida por profissionais que possuem profundo conhecimento dos processos, sistemas e cultura da entidade, devem executar atividades tais como avaliar tecnologias emergentes; analisar demandas internas de um ponto de vista global; avaliar riscos, controles, ética, qualidade, economicidade e eficiência. O auditor interno é um recurso valioso para todas as instâncias de administração e gerenciamento e uma empresa, inclusive para saber se os objetivos estabelecidos serão alcançados, bem como quanto a consistência dos controles internos e da governança corporativa.

A definição atual de Auditoria Interna, segundo o *Institute of Internal Auditors* (IIA) é:

"A auditoria interna é uma atividade independente e objetiva de avaliação (assurance) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia a organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança²".

A atividade de auditoria interna também desempenha um papel-chave na governança ao avaliar os riscos de reputação da organização, ao buscar entender a cultura ética dos colaboradores (incluindo empresas terceirizadas ou parceiras e, principalmente, fornecedores, que fazem parte da cadeia de

² Conforme tradução do IIA Brasil - disponível em <http://www.iiabrasil.org.br/new/IPPF.html>

produção) e ao dar ênfase à eficácia dos processos organizacionais no cumprimento das obrigações legais e regulamentares.

3 O Auditor Interno

3.1 Ética para o Auditor Interno

O conceito de ética profissional vai além de princípios morais e deve incluir normas de comportamento que tenham finalidades práticas que o profissional possa utilizar. Essas normas devem ser realistas e aplicáveis para que seu uso faça sentido.

O Instituto Americano de Contadores (*American Institute of Certified Public Accountants*), relacionado com o exercício profissional de auditoria, identificou que uma profissão precisa ser reconhecida não somente pela qualidade dos serviços que presta, mas também – na mesma extensão – por seus valores.

Os valores básicos associados à profissão são:

- Educação continuada e aprendizagem;
- Competência;
- Integridade;
- Atualização com questões amplas de negócios; e
- Objetividade.
- A alta administração confia nos auditores para auxiliá-la na gestão;
- Os auditores devem manter padrões elevados de conduta, honra e caráter, necessários ao exercício das funções;
- A unidade deve pautar-se por um código de ética que delineará os padrões de comportamento dos auditores.

Segundo o IIA, um código de ética é indispensável para o desempenho da profissão de auditor interno, já que sua atuação tem como base a confiança no alcance dos objetivos relacionados à administração, controle de riscos e aos processos de governança.

O código de ética adotado pelo IIA³ tem o propósito de promover uma cultura ética na profissão de auditor interno e é aplicável tanto a indivíduos como a entidades que prestam serviços de auditoria interna. Inclui dois componentes essenciais: os princípios e as regras de conduta, apresentados a seguir.

³ Disponível em <https://iibrasil.org.br//ippf/codigo-de-etica>

Os princípios relevantes para a profissão e a prática da auditoria interna são:

- Integridade - A integridade do auditor interno estabelece crédito e desta forma fornece a base para a confiabilidade atribuída a seus julgamentos;
- Objetividade - O auditor interno exibe o mais alto grau de objetividade profissional na coleta, avaliação e comunicação de informações sobre a atividade ou processo examinado. O auditor interno efetua uma avaliação equilibrada de todas as circunstâncias relevantes e não são indevidamente influenciados pelos interesses próprios ou de terceiros na formulação dos julgamentos;
- Confidencialidade - O auditor interno respeita o valor e a propriedade das informações que recebem e não divulga informações sem a autorização apropriada, a não ser em caso de obrigação legal ou profissional de assim procederem;
- Competência - O auditor interno aplica o conhecimento, habilidades e experiência necessárias na execução dos serviços de Auditoria Interna.

As regras de conduta descrevem as normas de comportamento a serem observadas pelo auditor interno. Essas normas auxiliam a interpretação e a aplicação prática dos princípios e orientam a conduta ética dos auditores internos.

- Integridade - o auditor interno:
 - a. Deve executar seus trabalhos com honestidade, diligência e responsabilidade.
 - b. Deve observar a lei e divulgar informações exigidas pela lei e pela profissão.
 - c. Não deve conscientemente tomar parte de qualquer atividade ilegal ou se envolver em atos impróprios para a profissão de Auditoria Interna ou para a organização.
 - d. Deve respeitar e contribuir para os objetivos legítimos e éticos da organização.

Os auditores internos têm a responsabilidade de observar as normas de conduta estabelecidas para a profissão. O IIA reconhece a importância da ética para o exercício da auditoria interna. Seu código de ética estabelece normas de conduta que exigem alto padrão de honestidade, objetividade, diligência e lealdade a ser observado pelos auditores internos. Orienta que os princípios

morais a serem seguidos pelos auditores devem ser formalizados, aceitos e praticados, tendo em vista que:

- Objetividade - o auditor interno:
 - a. Não deve participar de qualquer atividade ou relacionamento que possa prejudicar ou que presumidamente prejudicaria sua avaliação imparcial. Esta participação inclui aquelas atividades ou relacionamentos que podem estar em conflito com os interesses da organização.
 - b. Não deve aceitar nada que possa prejudicar ou que presumidamente prejudicaria seu julgamento profissional.
 - c. Deve divulgar todos os fatos materiais de seu conhecimento que, caso não sejam divulgados, podem distorcer o relatório apresentado sobre as atividades objeto da revisão.

- Confidencialidade - o auditor interno:
 - a. Deve ser prudente no uso e proteção das informações obtidas no curso de suas funções.
 - b. Não deve utilizar informações para qualquer vantagem pessoal ou de qualquer outra maneira fosse contrária à lei ou em detrimento dos objetivos legítimos e éticos da organização.

- Competência - o auditor interno:
 - a. Deve se comprometer somente com aqueles serviços para os quais possuam os necessários conhecimentos, habilidades e experiência.
 - b. Deve executar os serviços de Auditoria Interna em conformidade com as Normas Internacionais para a Prática Profissional de Auditoria Interna.
 - c. Devem melhorar continuamente sua proficiência, e a eficácia e qualidade de seus serviços.

Os funcionários da Auditoria Interna estão sujeitos às normas de conduta profissional estabelecidas para o funcionalismo da BB Previdência nos normativos internos.

3.2 Papel do Auditor Interno

Os auditores internos são empregados das organizações onde exercem o seu papel profissional. Desenvolvem uma atividade de avaliação dentro da

organização, que é denominada de auditoria interna e tem como objetivo atuar no fortalecimento da governança e na melhoria dos processos da organização

A extensão da função de auditoria interna abrange todas as fases das atividades de uma organização. É fácil constatar, portanto, que a natureza e a complexidade do ambiente organizacional em que a empresa está inserida e, por conseguinte, o trabalho do auditor requer:

- Adoção de modelo mental voltado à complexidade;
- Um conjunto variado de conhecimentos, mesmo que o trabalho do auditor esteja concentrado em áreas que exijam, precisamente, determinados conhecimentos específicos;
- Alto grau de determinação;
- Elevada capacidade de adaptação.

Tais requisitos se fazem necessários para que o auditor possa aprender rapidamente aspectos teóricos e práticos sobre as diversas atividades objeto de seu trabalho e assim possa conduzir satisfatoriamente todas as atribuições a ele confiadas.

3.3 Qualidades Inerentes ao Auditor Interno

Para o bom desempenho da função de auditor interno da BB Previdência, foram identificadas as seguintes características pessoais:

- Comprometimento profissional - capacidade de demonstrar interesse pelas atividades do cargo, determinação para atingir as metas estabelecidas e viabilizar o desenvolvimento pessoal e profissional;
- Comunicação - capacidade de expressar-se com fluência, segurança e objetividade, tanto por escrito quanto oralmente;
- Adaptabilidade - capacidade para assimilar e adaptar-se rapidamente às necessidades e exigências do meio, demonstrando flexibilidade e equilíbrio emocional;
- Iniciativa - capacidade de propor melhorias/soluções e agir oportunamente frente às situações;
- Postura ética - capacidade de agir com discrição, serenidade, retidão de princípios e imparcialidade, considerando os princípios éticos da Entidade;
- Senso crítico - capacidade de discernir e analisar logicamente os dados da realidade e efetuar o questionamento de si e dos outros;

- Visão sistêmica - capacidade de perceber o todo, as variáveis envolvidas num determinado problema, compreender suas relações e lidar com a dinâmica dos sistemas;
- Relacionamento interpessoal – capacidade de interagir com pessoas e grupos de forma empática, cordial e profissional, demonstrando facilidade em trabalhar em equipe;
- Coordenação - capacidade para conduzir grupos e acompanhar processos, atividades e procedimentos, para o alcance das metas estabelecidas;
- Dinamismo - habilidade para sugerir ou implementar ações/decisões agindo de forma tempestiva, ágil e efetiva;
- Liderança - habilidade para influenciar, orientar e desenvolver pessoas, proporcionando contexto motivador para o alcance dos objetivos estabelecidos.

Além desses fatores, outros podem contribuir sobremaneira para o exercício eficaz das funções do auditor, como autoconfiança, curiosidade, criatividade, senso de julgamento, rapidez de raciocínio abstrato e lógico, atenção a possíveis fontes de informações e suas relações, persistência nas investigações, modelo mental voltado para visão holística, predisposição para atuar em ambiente de complexidade.

3.4 Postura do Auditor Interno

O auditor interno contribui para a existência de um clima de cordialidade profissional entre seus colegas da organização. O sucesso do trabalho desenvolvido por um auditor depende de sua habilidade no trato com as pessoas, tanto quanto de sua capacitação técnica. É, portanto, responsabilidade do auditor derrubar as barreiras defensivas normalmente levantadas pelos interlocutores. Para conquistar respeito e confiança, é essencial que mantenha relações cordiais com as pessoas cujo trabalho examina. Atitudes negativas, além de dificultar o trabalho, em nada auxiliam na projeção de uma imagem de segurança em relação ao seu conhecimento e capacidade para avaliar rotinas, atividades e pessoas.

Sua palavra precisa ser colocada em tempo real, em local apropriado e de forma moderada – ele jamais deve usar ponderações com agressividade. As recomendações ou julgamentos devem justificar por si só a proposta do auditor no uso de seu senso profissional, baseado em suas experiências práticas e técnicas.

O equilíbrio pessoal deve ser cultivado e melhorado ao longo de sua carreira, buscando a obtenção de todas as evidências que substanciem sua opinião, traduzindo-a de forma consciente e impessoal.

Outros aspectos significativos relacionados à postura do auditor referem-se à sua independência no exercício da função e à necessidade de sigilo profissional.

A independência dos auditores internos deve ser definida nos estatutos de funcionamento, no regimento de auditoria interna e junto às áreas e funções da organização e às entidades externas (auditoria independente e organismos de fiscalização e controle).

A independência não reside no simples acesso aos documentos da empresa, mas na liberdade de programar, executar os trabalhos, elaborar conclusões e comunicar os resultados sem interferências. Além disso, os auditores internos devem adotar uma atitude imparcial e isenta e evitar qualquer conflito de interesses.

Segundo o IIA, o auditor interno fica impedido de desempenhar suas funções nas seguintes circunstâncias:

- Participação na diretoria ou órgãos administrativos da organização em que atua como auditor interno;
- Parentesco até segundo grau ou relação de interesse com diretores, sócios, membros dos conselhos deliberativo e fiscal ou de outros órgãos administrativos da organização;
- Participação societária ou acionária significativa, bem como participação em negócios da organização;
- Exercício de cargo ou função, fora da organização, contrário aos princípios que regem o exercício profissional da auditoria interna.

Quanto à observância da necessidade de sigilo profissional, ela decorre do fato de que, para desempenhar a função institucional de avaliação dos macroprocessos empresariais com foco em riscos, o auditor interno precisa ter acesso às informações confidenciais da organização.

Os postulados da ética profissional preveem que o auditor interno deve manter sigilo absoluto das políticas, diretrizes e estratégias estabelecidas pela organização. Só divulgará dados ou informações se expressamente autorizado

pela administração ou por determinação legal. Tal sigilo deverá ser mantido mesmo quando o auditor deixar de exercer funções de auditoria interna.

4 Auditoria Interna da BB Previdência

4.1 Governança

Criada em 1994 e administrada pelo Banco do Brasil, a BB Previdência – Fundo de Pensão Banco do Brasil atua como fundo de pensão multipatrocinado, situação em que diversos planos de benefícios de diferentes empresas – denominadas patrocinadoras – são administrados em conjunto, utilizando uma única infraestrutura, sem que haja vínculo ou responsabilidade entre eles.

Sua administração e organização são regidas pelo Estatuto Social, pelos Regimentos Internos e pelas disposições legais que lhe são aplicáveis.

Os princípios que irão nortear a forma de agir de todos os integrantes da BB Previdência são: ética, transparência, credibilidade, prudência, sustentabilidade, agilidade, competência, eficiência, potencial humano, inovação e governança.

As boas práticas de governança corporativa estão refletidas na macroestrutura organizacional da empresa e nas políticas de relacionamento com os patrocinadores, participantes, conselheiros, fornecedores e funcionários.

4.2 Posicionamento da Auditoria Interna na Organização

A Auditoria Interna está vinculada diretamente ao Conselho Deliberativo, conforme dispõe o Manual de Governança Corporativa. A Gerência desempenha papel fundamental no trabalho de acompanhamento do Conselho sobre a gestão.

A unidade está estruturada na forma de gerência, denominada Gerência de Auditoria Interna (Geaud). Seu posicionamento na macroestrutura da BB Previdência pode ser verificado na seguinte figura:



A Entidade adota o modelo das Três Linhas de Defesa, sendo que o controle estabelecido pelas próprias gerências representa a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pelas gerências são a segunda linha de defesa e a avaliação independente é a terceira. Cada uma dessas três “linhas” desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

Modelo de Três Linhas de Defesa



Adaptação da *Guidance on the 8th EU Company Law Directive* da ECIIA/FERMA, artigo 41

É responsabilidade do Gerente de Auditoria Interna a coordenação das três linhas de defesa e a integração com a Auditoria Externa e Reguladores, de tal forma a evitar lacunas ou sobreposição de funções. O Gerente deve buscar a efetividade do modelo, buscando a eficiência e eficácia das ações, assim como

garantir a adequada simetria de informações entre as partes integrantes do sistema.

4.3 Objetivos e estrutura da Auditoria Interna

A Geaud tem como principal objetivo assessorar a alta administração (Conselho Deliberativo, Conselho Fiscal e Diretoria Executiva) da BB Previdência e contribuir para o fortalecimento da governança corporativa e para o aprimoramento e eficácia dos processos de gestão. Para atingir esse objetivo, a área atua numa perspectiva proativa, com visão holística e independente.

A organização da Gerência, representada no organograma acima, está voltada para o cumprimento de suas responsabilidades e desempenho das funções que lhe foram atribuídas.

4.4 Responsabilidades

De acordo com o Manual de Organização da Entidade, são responsabilidades da Geaud:

- a. Responder pela qualidade, confiabilidade, adequabilidade e integridade na gestão dos controles e riscos dos processos da gerência;
- b. Assegurar que os negócios, produtos e serviços estejam sendo conduzidos de acordo com as leis e regulamentos aplicáveis e com as políticas e procedimentos internos;
- c. Assegurar o acompanhamento da legislação aplicável às atividades sob responsabilidade da gerência;
- d. Responder pela proposição, implementação e disseminação de ações voltadas para a prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção nos processos da gerência;
- e. Responder pela gestão dos riscos e controles associados aos processos da gerência;
- f. Assessorar o Conselho Deliberativo no desempenho de suas atividades;
- g. Atender a demandas do Conselho Fiscal;
- h. Assessorar a Diretoria Executiva em questões relacionadas a governança, riscos e controles;
- i. Responder pela proposição do Plano Plurianual de Auditoria Interna – PPAI- e do Plano Anual de Auditoria Interna - Paint;

- j. Responder pela realização de auditorias em processos com foco nos riscos, verificando a adequabilidade dos controles internos a partir da avaliação de sua qualidade, suficiência e cumprimento;
- k. Responder pelas avaliações sistemáticas e estruturadas que contribuem para a melhoria dos processos de gerenciamento de risco, de controle e de governança corporativa, inclusive no que diz respeito à prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção;
- l. Responder pelo acompanhamento das atividades de fiscalização e controle dos órgãos externos e da empresa de auditoria independente;
- m. Subsidiar os órgãos externos de fiscalização com informações, em articulação com as diretorias;
- n. Auxiliar no processo de contratação da auditoria independente;
- o. Responder pela certificação das recomendações de auditoria;
- p. Responder pelo acompanhamento e certificação de recomendações oriundas dos Conselhos Deliberativo e Fiscal, de órgãos de fiscalização, reguladores e auditoria externa;
- q. Subsidiar as auditorias internas e externas das patrocinadoras com informações, em articulação com as diretorias;
- r. Prospectar novas tecnologias de auditoria interna;
- s. Assegurar o acompanhamento da legislação aplicável às atividades sob responsabilidade da gerência.

As atividades da Auditoria Interna são:

- a) Auditar todos os processos da Entidade de acordo com o PPAI e Paint;
- b) Elaborar cronograma de trabalho da auditoria independente;
- c) Analisar a aderência dos processos da Entidade às leis, normas e regulamentos;
- d) Avaliar a Gestão de Riscos da Entidade, propondo ajustes e melhorias quando cabível;
- e) Avaliar o Sistema de Controles Internos – SCI – da Entidade, propondo ajustes e melhorias, quando cabível;
- f) Avaliar a governança da Entidade, propondo ajustes e melhorias, quando cabível;
- g) Elaborar relatório de auditoria interna para cada trabalho realizado;

- h) Elaborar proposta do PPAI e encaminhar para apreciação e aprovação do Conselho Deliberativo;
- i) Elaborar proposta do Paint e encaminhar para apreciação e aprovação do Conselho Deliberativo;
- j) Elaborar o Relatório Anual de Auditoria Interna - Raint, referente aos trabalhos realizados durante o ano;
- k) Propor escopo e avaliar propostas no processo de contratação de auditoria independente;
- l) Acompanhar o trabalho da auditoria independente e coordenar a solicitação e entrega de documentos requisitados;
- m) Fornecer insumos para o Relatório de Controles Internos do Conselho Fiscal e demais relatórios gerenciais;
- n) Elaborar relatório mensal de acompanhamento da implementação das recomendações apontadas pelas auditorias interna e externa;
- o) Certificar recomendações concluídas;
- p) Avaliar o processo de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção;
- q) Acompanhar legislação pertinente às atividades sob responsabilidade da gerência;
- r) Elaborar e implementar plano de ação de melhorias nos processos da gerência.

5 Auditoria Integrada

5.1 O que é?

A Auditoria Interna da BB Previdência adota métodos e técnicas com atuação fundamentada no pensamento complexo, que resulta da complementaridade entre a visão de mundo linear e a sistêmica.

A complexidade e suas implicações são as bases do denominado pensamento complexo, que vê o mundo como um todo indissociável e propõe uma abordagem multidisciplinar e multirreferenciada para a construção do conhecimento. Contrapõe-se à causalidade linear por abordar os fenômenos como totalidade orgânica. Para estudarmos qualquer fenômeno da natureza (incluindo os fenômenos do mundo corporativo), é necessário considerar todos

os seus aspectos, envolvendo as mais diversas disciplinas presentes no fenômeno, e que interagem entre si.

A Auditoria Interna tem como base o conceito de auditoria integrada, ou seja, é capaz de lidar, no plano interno, com a complexidade intrínseca dos macroprocessos da empresa e suas inter-relações e, na perspectiva externa, com a interface da organização com os ambientes regulatórios e com sua posição no ambiente competitivo em que atua.

Considera como funções vitais ou macroprocessos críticos da BB Previdência aqueles elementos essenciais de sua atividade produtiva, que viabilizam a realização de seus objetivos, evidenciam a importância da corporação e do valor que ela agrega à sociedade. Assim, todo processo ou subdivisão de Macroprocesso apresenta a seguinte configuração:

- Constitui um sistema aberto (interage com outros macroprocessos da empresa, com o meio ambiente, com fatores externos e cenários diversos);
- É constituído por um conjunto de objetivos, que dividem-se nas seguintes categorias: operacionais, de informação e de conformidade;
- Há riscos que ameaçam o cumprimento dos objetivos;
- É alimentado por insumos (recursos, entrada, matéria prima, fornecedores) necessários à viabilização dos objetivos definidos.



Figura 1 - Contínuo objetivo-risco-controle

A consecução desses objetivos apresenta, contudo, determinado grau de incerteza (risco), derivado de fatores internos ou externos ao processo. Como forma de minimizar esse risco faz-se necessária a implementação de controles; o que se dá a partir da identificação dos riscos existentes. Logo, a correta identificação dos riscos é condição imprescindível para a implementação dos controles necessários à sua mitigação e, por conseguinte, para alcance dos

objetivos organizacionais propostos. Em uma definição simplificada podemos ver que:

- Os riscos ameaçam os objetivos;
- Os controles internos mitigam os riscos; e
- A Auditoria Interna avalia a eficácia dos controles internos instituídos para mitigação dos riscos envolvidos.

Para cada objetivo identificado deve haver necessariamente a identificação do conjunto de riscos e controles a ele vinculados. Essas dimensões (objetivo – risco – controle) são subjacentes, integradas e sempre percebidas em conjunto.

A abordagem de auditoria integrada envolve avaliação sincronizada, multidisciplinar, independente e com enfoque sistêmico para verificação do gerenciamento dessa inter-relação entre objetivos, riscos e controles associados aos macroprocessos empresariais. Assim, os trabalhos de auditoria integrada devem estar voltados para exame do fluxo de trabalho em ambiente de complexidade, com vistas a orientar a percepção de fenômenos (manifestos ou latentes), cujas características indiquem desequilíbrio na inter-relação mencionada.

5.2 Pilares da Auditoria Integrada

A Auditoria Integrada está embasada em 2 pilares de atuação:

- Auditoria Baseada em Riscos – ABR;
- Abordagem por Macroprocessos Críticos.

5.3 Auditoria Baseada em Riscos - ABR

O primeiro pilar – ABR, amplia e aperfeiçoa o modelo de avaliação do risco, alterando a perspectiva da auditoria. A avaliação do risco pela auditoria interna permite identificá-lo, mensurá-lo e priorizá-lo para possibilitar o foco nas áreas auditáveis mais significativas. De acordo com a ABR, o auditor deve focar os processos de negócios numa perspectiva de risco, e não apenas como algo que está dentro de um sistema de controles. É um paradigma de olhar para frente. Uma auditoria baseada em riscos acrescenta mais valor à organização que uma auditoria focada nos controles.

Para agregar mais valor aos clientes e à organização, a auditoria interna deve passar do foco no passado para o foco no futuro. Com a sua atenção nos riscos, a auditoria fica mais abrangente, cobrindo toda a amplitude de aspectos que interessam à gestão.

A identificação e mapeamento de riscos associados ao universo auditável permitem a adoção de parâmetros de priorização, a obtenção de visão integrada do objeto avaliado, e a verificação dos controles a que está sujeito o processo.

No sentido de complementar esse modelo, foram identificadas oportunidades de aperfeiçoamento, que indicaram a possibilidade de ancoragem das avaliações em objetos auditáveis que apresentassem relevância e integrassem a própria organicidade da empresa, a fim de evitar a perda de esforço empreendido no mapeamento e a consequente limitação dos benefícios da curva de experiência.

5.4 Abordagem por Macroprocessos Críticos - AMC

Com o nível de complexidade emergente, a Auditoria Interna adotou o enfoque de atuação junto ao universo auditável, direcionando a atenção para as funções vitais (macroprocessos críticos) da Entidade. O Macroprocesso, concebido como função vital, apresenta as seguintes características:

- Representa os elementos da organicidade da empresa;
- Permite atuar de forma continuada e relacionada, em ciclos e rotações;
- Possibilita estabelecer priorização a partir dos rumos traçados nos documentos estratégicos;
- Viabiliza maior aproximação com os gestores que atuam sobre os macroprocessos empresariais;
- Apresenta, com simplicidade, a descrição de fenômenos complexos;
- Possibilita identificar padrões sistêmicos na perspectiva de integração;
- Sua avaliação pela Geaud pressupõe conhecimento técnico sistematizado e cumulativo sobre a constituição e suas inter-relações, potencializando os benefícios advindos da experiência.

Associada à visão de riscos, a abordagem por macroprocessos críticos possibilita uma definição de horizontes de longo prazo, assim como geração de

informações para diferentes níveis decisórios da organização. A implementação desta abordagem pautou-se nas seguintes premissas:

- Visão global e integrada do universo auditável;
- Modelos mentais orientados para a visão holística;
- Priorização dos objetos de maior relevância para a consecução dos objetivos da BB Previdência;
- Foco nos maiores riscos a que a empresa está exposta;
- Participação dos gestores e intervenientes em todos os estágios da auditoria.

Esse direcionamento garante proatividade, relevância e economicidade às atividades da Auditoria, uma vez que orienta o trabalho para avaliação de processos previamente selecionados, de acordo com a sua criticidade. Considera a visão sistêmica da organização em ambiente de complexidade e introduz, dessa forma, uma perspectiva ampliada, na medida em que avalia incertezas advindas do ambiente interno e externo e seus potenciais impactos sobre a organização.

6 Categorias de atividades de Auditoria Interna

6.1 Auditorias Programadas

As auditorias programadas têm como principal característica a autonomia da Auditoria Interna para propor os objetos que serão foco da avaliação, bem como a abordagem e a periodicidade dos trabalhos.

Os trabalhos de auditoria são realizados considerando-se ciclos de auditoria, definidos a partir da conclusão do mapeamento dos Macroprocessos Críticos, observado o seguinte:

- Ciclo de Auditoria – Intervalo de tempo estimado, dentro do qual a Gerência emite opinião conclusiva sobre todos os macroprocessos críticos da Entidade;
- Ciclo de Auditoria para Macroprocessos Críticos – Intervalo de tempo entre o início e a conclusão de uma avaliação de Macroprocesso Crítico. Pode ser considerado como o tempo que será consumido no período compreendido entre o momento de início de engajamento da força de trabalho e o seu momento final;

A definição dos trabalhos de auditoria para avaliação em cada ano leva em conta o Plano Plurianual vigente, a continuidade das ações iniciadas no ano anterior e a priorização dos principais riscos aos quais a BB Previdência possa estar exposta. As auditorias programadas contemplam:

6.1.1 Macroprocessos Críticos

Os Macroprocessos Críticos constituem o grupamento de maior relevância para a Auditoria Interna, uma vez que o seu conjunto representa os elementos constitutivos fundamentais da BB Previdência, cujo desvio ou exposição a determinados níveis de risco pode comprometer a eficácia organizacional, ou ameaçar sua perpetuação. Os Macroprocessos Críticos priorizados pela Auditoria Interna são definidos a partir de variáveis como: processos das operações e da gestão empresarial da BB Previdência; práticas de mercado; conhecimentos técnicos e experiência acumulada pela gerência.

As avaliações nos Macroprocessos Críticos são sistematizadas e integradas a fim de consolidar conclusões de auditoria para os diversos níveis de gestão, em um processo contínuo de aprendizado e de melhorias na gestão de riscos, controles e governança. Devido ao ambiente dinâmico das operações da BB Previdência, os elementos que constituem esses macroprocessos críticos devem ser periodicamente atualizados, por meio das atividades corporativas de mapeamento.

Os Macroprocessos Críticos utilizados pela Geaud são os seguintes:

- 1) Gestão da Estratégia
- 2) Gestão Orçamentária
- 3) Governança Corporativa
- 4) Gestão Previdencial
- 5) Gestão de Investimentos
- 6) Gestão de Portfólio de Produtos
- 7) Gestão de Relacionamento com Clientes
- 8) Gestão Contábil
- 9) Gestão Administrativa
- 10) Soluções em Tecnologia da Informação e Comunicação
- 11) Informações Gerenciais
- 12) Gestão de Riscos
- 13) Rotinas Atuariais

6.1.2 Auditorias Corporativas

Hoje, no ambiente político e de negócios, há um foco crescente na governança, gerenciamento de riscos e controle. São necessários sistemas de governança sólidos para assegurar que as organizações do setor privado atinjam seus objetivos e satisfaçam as expectativas das partes interessadas. Elas esperam que os conselhos e a gerência aceitem a responsabilidade pela implementação de práticas de governança apropriadas, colocando-os no centro das atenções quando se trata da questão. Ao cumprir suas responsabilidades de supervisão, a diretoria olha para a função de Auditoria Interna para fornecer avaliações sobre as práticas de governança da organização.⁴

6.1.3 Auditorias Obrigatórias

Faz parte do universo auditável trabalhos que estão estabelecidos em normativos internos e externos, tais como:

- Relatório de Controles Internos - RCI
- Acompanhamento de fiscalizações da Previc e órgãos reguladores
- Acompanhamento da Auditoria Externa
- Resolução CGPAR 9/2016, de 10.05.2016

6.1.4 Demandas Extraordinárias

Além dos trabalhos de auditorias programadas e obrigatórias, a Geaud recebe demandas eventuais, cujas horas de trabalho devem estar incluídas no planejamento. Demandas do Conselho Deliberativo (CD), da Diretoria Executiva (Direx) e do Conselho Fiscal (CF).

6.1.5 Projetos

Projetos representam um conjunto de atividades planejadas e coordenadas para se alcançar melhorias nos processos internos da auditoria interna.

⁴ Extraído de <https://iiabrasil.org.br//ippf/orientacoes-suplementares> - “Assessing Organizational Governance in the Private Sector.”

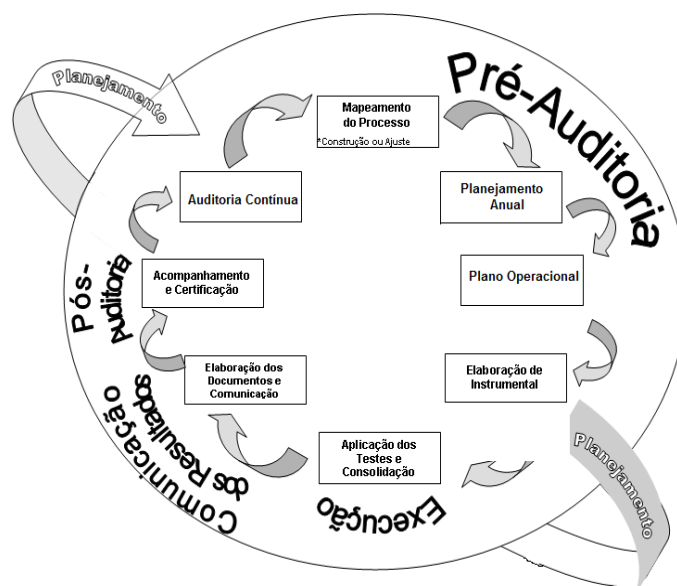
Parte 2 - Metodologia de Auditoria Interna

1 Processo de Auditoria

1.1 Princípios do Processo

O processo de auditoria, no contexto da auditoria integrada, é composto pelo seguinte conjunto das fases:

- Planejamento;
- Pré-auditoria;
- Execução;
- Comunicação de resultados;
- Pós-auditoria.



Essas fases são como elos de uma corrente interativa. Possuem entre si uma relação circular sendo retroalimentadas pelas fases subsequentes. Como exemplo, o conhecimento obtido no mapeamento de um determinado macroprocesso poderá ser atualizado quando da elaboração de um Plano Operacional ou mesmo quando finalizada uma pós-auditoria.

necessário um planejamento Plurianual (Plano Plurianual da Auditoria Interna – PPAI), que abrange os trabalhos necessários para avaliar todos os macroprocessos da Entidade, considerando o escopo desejado e a estrutura disponível. O horizonte de tempo considerado para avaliação de todo o universo auditável é de três anos.

O Planejamento Anual da Auditoria Interna – Paint, que tem um horizonte de tempo anual, estabelece os trabalhos que serão realizados, sua duração e a equipe responsável por sua execução. Ele é construído a partir do Plano Plurianual, bem como da avaliação de risco efetuada pela Auditoria Interna. Os processos avaliados com maior risco deverão ser auditados anualmente.

1.3 Pré-Auditoria

1.3.1 O que é?

A norma IPPF 2200⁵ estabelece o seguinte:

Norma 2200 – Planejamento do Trabalho de Auditoria

Os auditores internos devem desenvolver e documentar um planejamento para cada trabalho de auditoria, incluindo os objetivos, o escopo, o prazo e a alocação de recursos do trabalho.

Ainda sobre o planejamento dos trabalhos de auditoria, a norma 2201 declara:

⁵ IPPF – Normas Revisadas – vigência a partir de 1 de janeiro de 2017.

Norma 2201 – Considerações sobre o Planejamento

No planejamento dos trabalhos de auditoria, os auditores internos devem considerar:

- Os objetivos da atividade que está sendo revisada e os meios pelos quais a atividade controla seu desempenho;
- Os riscos significativos para a atividade, seus objetivos, recursos e operações e os meios pelos quais o impacto potencial dos riscos é mantido em um nível aceitável;
- A adequação e a eficácia dos processos de governança, gerenciamento de riscos e controles da atividade, comparativamente a uma estrutura ou modelo compatível; e
- As oportunidades para se fazer melhorias significativas nos processos de governança, gerenciamento de riscos e controles da atividade.

O planejamento do trabalho é feito na fase de pré-auditoria. Os objetivos e escopo definidos no Paint devem ser revistos, a partir de revisões da avaliação de risco feito pela administração da Entidade após a aprovação do Paint. Outras considerações incluem a atividade prévia de avaliações de risco e reportes de auditoria com relação à área sob revisão. O planejamento das ações de auditoria constitui-se em um processo dinâmico e contínuo para o sucesso do trabalho do auditor interno, devendo este estar alinhado às prioridades da Instituição. Deve ser realizado de modo a assegurar que uma auditoria de alta qualidade seja conduzida de maneira econômica, eficiente, efetiva e com tempestividade. Pressupõe adequado nível de conhecimento sobre as atividades, os fatores econômicos, legislação aplicável e as práticas operacionais da entidade, e o nível geral de competência de sua administração.

Para estabelecer os objetivos da atividade, os auditores internos geralmente identificam os dados exigidos no escopo do trabalho de auditoria e comunicam o escopo à administração da área sob revisão, concedendo à administração tempo adequado para preparação. Os auditores internos também se comunicam com a administração da área sob revisão para garantir a disponibilidade do pessoal da área responsável pelo processo auditado no início do processo.

Uma vez estabelecidos os objetivos e escopo do trabalho de auditoria, ambos devem ser detalhados e declarados formalmente, definindo os limites nos quais os auditores internos trabalharão. O documento utilizado para tal fim é o Plano Operacional, cujo modelo pode ser acessado na rede da Geaud. O Plano

Operacional deve suficientemente discutido no âmbito da Geaud e ser aprovado pelo Gerente de Auditoria, antes do início do trabalho de campo.

Durante a pré-auditoria pode haver a identificação de vulnerabilidades na gestão dos controles e riscos ou na governança empresarial, as quais devem receber imediato tratamento pela Auditoria Interna e podem ser objeto, inclusive, de emissão de recomendações e de acompanhamento específicos.

Excepcionalmente, a pré-auditoria pode ser suficiente para assegurar manifestação conclusiva e exaurir nesta etapa os procedimentos de execução, situação em que o processo de auditoria deve ser remetido à etapa de comunicação de resultados.

1.3.2 Objetivos

Norma 2210 – Objetivos do Trabalho de Auditoria

Os objetivos devem ser estabelecidos para cada trabalho de auditoria.

Normas Revisadas, com vigência a partir de 1 de janeiro de 2017.

Os principais objetivos desta fase são:

- Prover conhecimento suficiente sobre os elementos integrantes do processo e respectivos objetivos, riscos e controle associados;
- Identificar os intervenientes diretos e indiretos no processo, unidades organizacionais e sistemas de informação de suporte;
- Identificar e selecionar, por meio da aferição de criticidade, aqueles elementos críticos que representam a quantidade suficiente de pontos para avaliação do processo;
- Integrar, de forma sistêmica, os elementos do processo sob referência com demais objetos do universo auditável (estabelecer vinculações horizontais);
- Potencializar o escopo do trabalho ao considerar as diversas abordagens (visões) pretendidas sobre o objeto;
- Elaborar testes e definir os elementos representativos que serão testados;
- Definir as técnicas/procedimentos amostrais a serem empregados na escolha dos elementos a serem testados: censo, onde serão examinados todos os elementos de uma determinada população;

- Amostragem (estatística ou não estatística), onde será testado um conjunto menor de elementos a fim de emitir determinada conclusão de auditoria;
- Mensurar o tempo necessário para a conclusão da auditoria e sincronizar as ações e resultados esperados;
- Otimizar a alocação de recursos.

1.3.3 Levantamento e análise de dados

O levantamento e análise de dados contemplam a busca e o registro ordenado e sistematizado de dados para conhecer/atualizar as informações acerca do objeto de auditoria, relativamente aos ambientes interno e externo.

Existem várias áreas em que a auditoria de dados pode ser aplicada. Com base nesta lista, apresenta-se abaixo uma variação contendo possibilidades mais especificamente associadas ao controle externo:

- Análise exploratória: análise preliminar dos registros armazenados na base de dados. Essa atividade pode apoiar o processo de planejamento da auditoria, uma vez que poderá indicar que áreas ou transações, em função de risco e materialidade, deverão ser objeto da execução de procedimentos adicionais de auditoria.
- Teste e avaliação de controles: verificação de conformidade dos registros às regras de negócio. A auditoria de dados permite que para um dado processo 100% das transações sejam verificadas, reduzindo o risco de análises incompletas em razão de amostras estatísticas mal planejadas.
- Detecção de fraudes: análise de transações para identificar indícios de fraude. As possibilidades dessa análise dependem da área de negócio sob fiscalização e da experiência do auditor. Algumas das verificações mais comuns são: análise das transações mais vultosas; sumarização da execução de registros por usuário; análise de incompatibilidade entre o cargo ou função do usuário e as transações por eles desempenhadas, e outras.
- Análise de trilhas de auditoria e logs de acesso: tabelas de logs e de trilhas de auditoria frequentemente contém milhões de registros, dificultando seu uso e análise. Uma boa ferramenta de auditoria de dados, pode, contudo, permitir que os logs sejam uma importante fonte de informações para o auditor.

Deve ser realizado, no que for aplicável, em conjunto com a área responsável, para que seja alcançado maior comprometimento dos gestores e maior fidedignidade das informações.

Nesta fase é importante também efetuar levantamento de missões anteriores de auditoria, bem como de fiscalizações efetuadas por órgãos externos, inclusive da auditoria externa.

1.3.4 Mapeamento e Mapas

O conhecimento dos objetos, obtido na pré-auditoria, é estruturado por meio de mapas e registrado em roteiros de auditoria. Deve ser sistematicamente atualizado durante as demais fases do processo de auditoria.

O mapeamento não impõe limites rígidos aos macroprocessos empresariais, apenas fronteiras de contorno. A partir do trabalho de mapeamento são produzidos mapas de processos, que são as representações estruturadas do conhecimento do fluxo de trabalho dos objetos do universo auditável.

O mapa deve ser elaborado pela Gerência de Auditoria, a partir do mapeamento efetuado pelos gestores dos processos e de levantamentos efetuados pela própria Geaud, e as informações nele contidas devem ser armazenadas na rede da Auditoria Interna, onde estão detalhadamente registrados o macroprocesso e seus elementos, objetivos, riscos e controles, intervenientes, pontos críticos identificados e vinculações sistêmicas com demais macroprocessos críticos. Além disso, os elementos do macroprocesso crítico devem ser classificados de acordo com sua criticidade, por meio da matriz de processos a serem avaliados.

O mapa dos processos fundamenta a integração das informações no escopo de cada macroprocesso crítico (sentido vertical) e nas relações com outros processos da empresa (sentido horizontal).

1.3.5 Amostragem

Em trabalhos de auditoria nos quais já se tenha definido os respectivos objetivos e formulados os testes, deve-se verificar se será necessário fazer um levantamento de dados e se tal providência exigirá apurar informações quantitativas. Se for suficiente apenas verificar se algum fenômeno ocorre ou não, sem necessidade de mensurar tal ocorrência, os dados podem ser coletados por critérios de conveniência do auditor, após o que ele deve fazer sua análise qualitativa à luz do objetivo do teste.

Quando for necessário conhecer todas as ocorrências ou repetições possíveis de um fenômeno aleatório, deve-se analisar sua população, o conjunto

total de dados de um universo auditável. Quando trabalhamos com todo o universo, estamos realizando um censo. Em um censo os resultados possuem precisão absoluta.

Caso não seja possível operacionalizar um censo, o auditor deve utilizar uma amostra estatística. A amostra é um subconjunto da população, a partir do qual se infere conclusões relativas ao todo, com determinado grau de certeza (nível de confiança) e margem de erro. A margem de erro é um elemento estatístico que expressa a quantidade de erro de amostragem aleatória em um resultado de uma pesquisa. Quanto maior a margem de erro, menos confiança temos que os resultados da pesquisa correspondam aos valores "verdadeiros"; ou seja, os valores para a população inteira.

Esses parâmetros são medidas usadas para descrever sumariamente uma característica numérica da população. A média (μ), o Total (T) e as proporções (p) são os parâmetros populacionais que mais comumente desejamos estimar.

1.3.6 Instrumental de Auditoria

O Instrumental de auditoria é a ferramenta utilizada para testar os elementos sob avaliação. Armazena os apontamentos, anotações e informações obtidas durante o exame realizado pelo auditor e orienta os pontos sobre os quais são aplicados os testes de auditoria. Tecnicamente, o instrumental de auditoria é composto pelo Papel de Trabalho - PT. Contempla todos os testes preparados de forma manual, eletrônica ou por outro meio que represente a percepção e o conhecimento do auditor sobre o objeto avaliado.

1.3.6.1 Papel de Trabalho - PT

Todas as conclusões e afirmações expressas pelo auditor devem estar consubstanciadas em um Papel de Trabalho. O PT deve conter, quesitos para todos os elementos do macroprocesso que serão auditados, os objetivos pretendidos com a aplicação dos testes, orientações sobre seu preenchimento, indicação da técnica de auditoria mais adequada para a obtenção das respostas, as diferentes opções de resposta (data, lista, texto, "Sim/Não/Prejudicado", entre outros) e a necessidade de justificativas e/ou comentários para os assinalamentos, se for o caso, de modo a facilitar a compreensão do motivador do instrumental e suas implicações para o trabalho.

1.3.6.2 Papel de Trabalho Auxiliar – PT Auxiliar

O PT auxiliar é utilizado para tabular os dados da população ou amostra que está sendo analisada. Normalmente este instrumento tem uma linha para

cada elemento populacional/amostral analisado, sendo o resultado consolidado utilizado como subsídio para preenchimento de um outro PT.

1.3.6.3 Orientações Gerais

Os papéis de trabalho não devem se limitar a um simples *checklist* e por ocasião de sua elaboração devem ser consideradas as premissas de avaliação da adequabilidade do gerenciamento de riscos, controles e governança, sob aspectos de conformidade e gestão, inclusive quanto a possíveis causas dos fenômenos a serem eventualmente observados. Além disso, os PT devem observar os requisitos de qualidade para redação de documentos adotados pela Geaud. O zelo com a confidencialidade dos papéis de trabalho deve ser permanente, pois além de o instrumental suportar as conclusões de auditoria, resguarda o auditor interno, ao evidenciar seus exames e constatações. Cabe à Instituição mantê-los sob sua guarda e garantir o acesso a entidades de fiscalização.

1.4 Execução

Norma 2310 – Identificação das Informações

Os auditores internos devem identificar informações suficientes, confiáveis, relevantes e úteis para cumprir os objetivos do trabalho da auditoria.

Interpretação:

Informação suficiente é factual, adequada e convincente de forma que uma pessoa prudente e informada chegaria às mesmas conclusões que o auditor. Informação confiável é a melhor informação possível de ser obtida através da utilização de técnicas de auditoria apropriadas. Informação relevante dá suporte às observações e recomendações do trabalho da auditoria e é consistente com os objetivos do trabalho da auditoria. Informação útil auxilia a organização a atingir as suas metas.

Normas Revisadas, com vigência a partir de 1 de janeiro de 2017.

1.4.1 O que é?

A execução da auditoria é a fase do processo destinada à realização do trabalho em campo. A ênfase das ações deve estar direcionada para a coleta, análise, interpretação e documentação das evidências que suportarão as conclusões de auditoria.

O conjunto de procedimentos desta fase é parametrizado pelo contido no respectivo Plano Operacional e deve estar focado no exame dos processos, com foco nos riscos aos quais eles podem estar expostos.

A execução de auditoria deve ser antecedida de comunicação aos gestores intervenientes e da adoção de procedimentos que assegurem a disponibilização tempestiva dos recursos necessários à consecução dos objetivos do trabalho.

A realização de reunião inicial com funcionários das gerências sob avaliação, para a execução de auditoria, deve esclarecer o escopo dos trabalhos, os canais de comunicação, a metodologia adotada pela Geaud e os resultados esperados.

1.4.2 Aplicação de testes

A aplicação de testes é orientada pelos papéis de trabalho e neles são armazenadas as informações resultantes, fundamentando as conclusões de auditoria.

As evidências coletadas devem ser registradas de forma a permitir a pronta recuperação das informações, seja para servir de trilha na reconstituição das conclusões obtidas pela auditoria, para subsidiar entidades de fiscalização e controle, ou ainda para resguardar o auditor quanto à fidedignidade das informações por ele registradas.

A aplicação de testes deve considerar as diferentes técnicas de auditoria (observação direta, entrevista, exame documental, conferência física, entre outras previstas) e permitir ao auditor a formação de convicção quanto à adequação da gestão de riscos, controles e da governança.

1.4.3 Indicadores

Durante o processo de execução são identificados indicadores de auditoria com foco no gerenciamento dos riscos, dos processos de negócio e atividades de controle críticas e têm como objetivo melhorar a eficiência das operações na Entidade, identificando e avaliando riscos de maneira tempestiva e provendo rapidamente informações críticas a Alta Administração para uma melhor tomada de decisão. Esses indicadores serão utilizados para a construção dos testes de auditoria contínua.

1.4.4 Achados de Auditoria

Achados de auditoria são os fatos relevantes constatados, que devem ser registrados e encaminhados para tratamento específico pelo respectivo responsável, em função da criticidade.

O conjunto de fatos relevantes percebidos deve ser objeto de estudo que permita identificar a relação de causa x efeito entre eles. A emissão de recomendação de auditoria deve então direcionar as ações corretivas para os fatos responsáveis por desencadear (causar) os demais fatos observados, otimizando a ação de auditoria.

Os achados de auditoria (constatações) são classificados como falha ou fragilidade e são suportados por evidências obtidas por meio dos testes de auditoria. As evidências coletadas devem ser suficientes, válidas e relevantes para sustentar as conclusões de auditoria.

Todos os achados de auditoria devem ser classificados quanto à sua criticidade e abrangência, para possibilitar a visualização de seus impactos e sua irradiação no ambiente organizacional e facilitar o gerenciamento dos procedimentos utilizados para mitigação dos efeitos indesejáveis a eles associados.

Essa classificação deve ser discutida previamente com o gestor. Devem ser esclarecidas suas funções e consequências, inclusive no que diz respeito ao estabelecimento de prazos previstos para cumprimento de eventuais recomendações, bem como no que concerne à alçada para eventual prorrogação de prazo dessas recomendações.

A criticidade das falhas e fragilidades é classificada de acordo com sua relevância (impacto x probabilidade), podendo ser: A - risco alto; B - risco médio-alto; C - risco médio-baixo; ou D - risco aceitável.

Quando da percepção de fatos cujas características sugiram necessidade de apuração de irregularidades, tais fatos devem ser submetidos à avaliação do Gerente de Auditoria. Confirmada a necessidade de apuração de irregularidade, devem ser adotados os procedimentos descritos no Código de Ética da Entidade.

1.4.5 Registros de Fragilidade e Lista de Falhas

São documentos que descrevem uma situação-problema, suas características, evidências, causas, consequências ou potenciais efeitos e seu impacto no resultado e/ou na reputação da empresa, assim como as recomendações para mitigação dos riscos associados às constatações, se for o caso.

Possuem a função de provocar a tomada de ações corretivas ou otimizadoras em relação à gestão de riscos, controles e governança corporativa. Nas evidências/exemplos devem ser registradas informações suficientes para a sua caracterização e adoção de medidas corretivas, sem, no entanto, permitir a

terceiros externos à BB Previdência identificar aspectos sob tutela do sigilo das informações.

Para as fragilidades sempre serão indicadas recomendações específicas para sua regularização e serão acompanhadas na fase de pós-auditoria pelo sistema de Auditoria. Para as falhas não serão emitidas recomendações.

1.4.6 Recomendação

É a indicação de solução, acordada entre o auditor e o gestor, com o propósito de sanar as fragilidades identificadas e mitigar os riscos decorrentes.

As avaliações e recomendações feitas pela auditoria interna devem estar alinhadas ao direcionamento estratégico da organização e se destinam a aperfeiçoar controles internos, normas e procedimentos, além de identificar riscos e sugerir controles para mitigá-los. Essas avaliações serão utilizadas pela gestão e pelo Conselho Deliberativo – uma das responsabilidades do conselho é a de supervisionar as decisões tomadas pelos gestores e garantir o alinhamento de tais decisões aos princípios, à missão, à visão e aos valores da organização.

A recomendação de auditoria deve ser emitida para o principal gestor responsável pela solução do problema identificado, e indicar “o que” deve ser feito e não “como” fazer.

Obs.: O vencimento das recomendações de auditoria emitidas deve estar preferencialmente compreendido entre os dias 01 e 25 de cada mês.

A premissa da responsabilidade pela implementação de recomendações considera a existência de um único principal responsável.

A recomendação deve ter foco no tratamento de suas causas, para sanear as vulnerabilidades dos processos avaliados. Deve-se atentar para a pertinência e a relevância das recomendações e evitar pontos insignificantes. Devem ser propostas apenas soluções possíveis de serem implementadas e que contribuam para a melhoria do processo, com aperfeiçoamento da gestão e da governança.

As constatações devem ser discutidas com o gestor, na medida em que forem identificadas, e os prazos acordados para implementação devem ser compatíveis com a criticidade da fragilidade encontrada, com a complexidade das alterações necessárias nos controles e com os recursos envolvidos.

Depois de firmada convicção, os problemas identificados e as soluções propostas devem ser imediatamente formalizados e registrados, de modo a propiciar tempestividade e transparência às informações. Após a implementação

da recomendação pelo responsável, a Auditoria Interna fará um trabalho de certificação dessa implementação.

1.4.6.1 Recomendação tipo plano de ação

A recomendação do tipo plano de ação envolve a confecção de plano de ação para fazer frente às fragilidades identificadas e mitigar os riscos decorrentes, observadas as normas sobre recomendação.

Somente recomendações que demandem estudos mais aprofundados, em função da complexidade da situação-problema identificada, serão passíveis de tratamento pela via do plano de ação.

O plano de ação é registrado pelo gestor diretamente no Sistema de Auditoria quando da implementação da Recomendação tipo plano de ação. É analisado pelo auditor responsável pelo acompanhamento, considerando os aspectos de pertinência e suficiência das ações sugeridas e prazo para implementação.

As orientações para registro do plano de ação na Intranet, pelos gestores, estão disponíveis no Manual de Procedimentos e Rotinas: Acompanhar Recomendações de Auditoria.

No que se refere à implementação e certificação destas recomendações, aplicam-se as mesmas instruções das demais recomendações. No caso de não-certificação, a situação será alterada para "Vincenda" ou "Vencida", de acordo com a data que restar pactuada (o sistema excluirá a data da implementação registrada).

Excepcionalmente, será possível propiciar ajustes, pelo Gestor responsável pela implementação do plano de ação, das ações propostas, sem que a situação "A Certificar" seja alterada para "Vincenda" ou "Vencida".

1.5 Comunicação de Resultados

Norma 2410 – Critérios para a Comunicação

As comunicações devem incluir os objetivos e o escopo do trabalho de auditoria, assim como as conclusões, recomendações e planos de ação aplicáveis.

Normas Revisadas, com vigência a partir de 1 de janeiro de 2017.

É a etapa do processo de auditoria que apresenta as conclusões do trabalho de auditoria. A comunicação final dos resultados do trabalho deve incluir

as conclusões aplicáveis, assim como as recomendações e/ou planos de ação aplicáveis. Quando apropriado, a opinião dos auditores internos deve ser fornecida. Uma opinião deve levar em consideração as expectativas da alta administração, conselho e outras partes interessadas e deve estar suportada por informação suficiente, confiável, relevante e útil.

Considera a estrutura da informação em diferentes níveis e visões, sua oportunidade e a customização adequada aos interessados nos diversos segmentos da Entidade.

A comunicação de resultados é materializada pelos seguintes documentos: Relatório de Auditoria, Registro de Fragilidade e Lista de Falhas e Súmula de Trabalho de Auditoria.

1.5.1 Relatório de Auditoria

O Relatório de Auditoria é o documento formal e técnico por meio do qual a Geaud comunica os resultados dos trabalhos aos gestores do processo e à Diretoria. Apresenta aos gestores conclusões sobre a suficiência da gestão dos riscos e controles e da governança dos processos sob sua responsabilidade. Deve manter relação entre a conclusão de auditoria e o objetivo estabelecido no Plano Operacional e integrar as informações geradas para obtenção de conclusões para os níveis superiores: Macroprocesso Crítico/Processo (se for o caso). Deve também estar embasado em documentação formal e evidências que sustentem suas afirmativas.

O Relatório deve representar a opinião/conclusão do trabalho e ao ser elaborado deve atentar para:

- Erros e omissões significantes.
- Linguajar técnico demais ou com muito jargão.
- Observações e recomendações que não estejam bem formuladas.
- Não reconhecer o desempenho satisfatório.
- Omitir ou não explicar limitações de escopo.
- Emitir relatórios atrasados ou entregá-los a partes inapropriadas.

A comunicação com a administração é um processo contínuo ao longo do trabalho. A atividade de auditoria interna agrega valor ao desenvolver comunicações (tanto verbais quanto escritas) que provoquem mudanças positivas na organização. Ao comunicar os resultados do trabalho, os auditores internos são encorajados a reconhecer o desempenho satisfatório e incluir quaisquer declarações sobre limitações de distribuição e/ou uso dos resultados.

1.5.2 Súmula de Trabalho de Auditoria

A Súmula de Trabalho de Auditoria (Súmula) é o documento, em formato executivo, pelo qual a Geaud comunica formalmente e de forma sucinta o resultado de seus trabalhos aos Conselhos Deliberativo e Fiscal.

O documento deve ser elaborado a partir do modelo aprovado pelo Conselho Deliberativo, obedecendo a padronização de formato (tipo e tamanho da fonte) e de cores, e devem ser observados os critérios de oportunidade, economicidade e os requisitos de qualidade de apresentação e conteúdo.

A Súmula deve ser validada pelo Gerente de Auditoria e encaminhada à Diretoria e aos Conselhos Deliberativo e Fiscal.

1.6 Pós Auditoria

Norma 2500 – Monitoramento do Progresso

O executivo chefe de auditoria deve estabelecer e manter um sistema para monitorar a disposição dos resultados comunicados à administração.

Normas Revisadas, com vigência a partir de 1 de janeiro de 2017.

As recomendações de auditoria devem ser acompanhadas, quanto ao seu cumprimento. Após o gestor responsável por sua implementação comunicar à Auditoria Interna a implementação da recomendação, a Geaud deve proceder uma avaliação da efetividade das ações do gestor. Esta avaliação é a certificação da recomendação, e deve ser registrada no sistema de acompanhamento da auditoria, na intranet da Entidade.

2 Auditoria Contínua

A abordagem da auditoria interna para avaliar a eficácia da gestão de riscos e controles tem sido historicamente retrospectiva, com testes de controles realizados em base cíclica - muitas vezes meses após as atividades de negócios terem ocorrido. Dois fatores estão impulsionando os esforços para modificar esta abordagem:

- a) A necessidade das organizações acompanharem o ritmo dos negócios, respondendo mais oportunamente às taxas aceleradas de mudança e aos riscos emergentes.
- b) Os avanços na tecnologia permitindo as avaliações contínuas e até em tempo real dos riscos e controles.

A auditoria contínua tem como objetivo avaliar controles e riscos automaticamente em bases contínuas, de forma a identificar exceções e anomalias, tendências e indicadores de riscos e estabelecer rotinas que:

- a. Detectem erros potenciais;
- b. Inibam comportamentos e eventos inapropriados;
- c. Reduzam ou evitem perdas financeiras; e
- d. Verifiquem a aderência às leis existentes, normas e procedimentos.

2.1 Estratégia de Auditoria Contínua

Os testes de auditoria contínua devem ser implementados naqueles processos que tenham sido mapeados e analisados pela Auditoria Interna. A auditoria contínua deve ser utilizada para:

- Monitoramento dos riscos mais críticos e ainda não suficientemente mitigados;
- Detecção de *outliers* – transações que estejam acentuadamente fora dos padrões; e
- Tendências futuras apontadas pelos indicadores do processo, que podem representar uma perda para a Entidade.

Os processos que serão auditados por meio da auditoria contínua devem ter seus trabalhos iniciados logo na abertura do ciclo anual de auditoria. No levantamento dos indicadores, os sistemas e fluxo de dados devem ser mapeados ou revistos, conforme o caso. O fluxo de cálculo e apuração dos indicadores devem ser devidamente documentados, assim como a forma de comunicação de resultados. Os testes de auditoria contínua devem ser executados até o momento em que a auditoria interna avalie que os riscos monitorados estão adequadamente mitigados. Os testes executados podem ser, então, repassados aos gestores (primeira camada), para que eles mesmos façam o monitoramento desses riscos.

2.2 Obtenção dos dados

O acesso aos dados deve ser feito a partir das bases de dados corporativas, com acesso direto da Auditoria Interna. Após a identificação dos indicadores e dos dados a serem analisado é necessário fazer verificações de integridade e validade e preparar rotinas de teste. Os dados para cálculo dos indicadores devem ser copiados para uma área de acesso exclusivo da equipe de auditores.

Os testes realizados, quando possível, devem ser feitos com a população inteira, pois aumenta a eficácia da busca por erros e transações incomuns.

Durante a execução, os “*scripts*” devem ser pré-definidos, deve haver o acompanhamento da execução do cálculo e por fim, a validação do cálculo. As rotinas analíticas e os resultados que elas geram devem ser periodicamente revisados. Isso ajuda a garantir que as conclusões obtidas a partir do uso da análise de dados possam ser usadas com confiança e que quaisquer erros no levantamento dos dados sejam identificados e corrigidos, ou que as conclusões obtidas a partir desses resultados não sejam errôneas.

2.3 Indicadores de Auditoria Contínua

Devem ser avaliados quais são os principais indicadores e “agentes” que oferecem mais riscos à Entidade e considerar a relação sobre o Custo x Benefício. É necessário classificar e priorizar os principais riscos e o nível de automação dos indicadores. A periodicidade do cálculo também deve estar definida.

Os indicadores devem ser avaliados quanto à criticidade dos riscos relacionados e quanto aos objetivos estratégicos da Entidade.

2.4 Comunicação de Resultados e Monitoramento

Os resultados obtidos devem ser comunicados através de relatórios ou publicados em painéis de indicadores, disponíveis aos gestores e a alta administração da Entidade.

Uma vez que o programa de auditoria contínua tenha sido estabelecido, com a auditoria interna produzindo relatórios regularmente apontando ineficácia dos controles e/ou possíveis erros, fraude ou não conformidade, o próximo passo lógico é que a administração assuma o monitoramento de seus próprios processos.

BB PREVIDÊNCIA